



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/869,966	09/14/2001	Louis Guillou	9320.133USWO	4277
23552	7590	03/16/2005	EXAMINER	
MERCHANT & GOULD PC P.O. BOX 2903 MINNEAPOLIS, MN 55402-0903			SIMITOSKI, MICHAEL J	
			ART UNIT	PAPER NUMBER
			2134	
DATE MAILED: 03/16/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/869,966

Applicant(s)

GUILLOU ET AL.

Examiner

Michael J Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 14 September 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 14 September 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 9/14/01.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. The preliminary amendment of 9/14/2001 was received and considered.
  - a. Note: the preliminary amendment (p. 6) introduces new claims 3 and 9, however, claims 3 and 9 already exist in the claims. Therefore, the newly added claims 3 and 9 were not considered.
2. The IDS of 9/14/2001 was received and considered.
3. Claims 1-12 are pending.

### ***Drawings***

4. The drawings are objected to because the specification does not describe the drawings in such a way as to enable one of ordinary skill in the art to understand the drawings.

### ***Specification***

5. The disclosure is objected to because it does not conform with standard U.S. practice. Further, the disclosure makes no reference to the drawings.
6. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

### **Arrangement of the Specification**

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

- (a) TITLE OF THE INVENTION.
- (b) CROSS-REFERENCE TO RELATED APPLICATIONS.

Art Unit: 2134

- (c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
- (d) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or  
REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)
- (e) BACKGROUND OF THE INVENTION.
  - (1) Field of the Invention.
  - (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
- (f) BRIEF SUMMARY OF THE INVENTION.
- (g) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
- (h) DETAILED DESCRIPTION OF THE INVENTION.
- (i) CLAIM OR CLAIMS (commencing on a separate sheet).
- (j) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
- (k) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

#### **Content of Specification**

- (a) Title of the Invention: See 37 CFR 1.72(a) and MPEP § 606. The title of the invention should be placed at the top of the first page of the specification unless the title is provided in an application data sheet. The title of the invention should be brief but technically accurate and descriptive, preferably from two to seven words may not contain more than 500 characters.
- (b) Cross-References to Related Applications: See 37 CFR 1.78 and MPEP § 201.11.
- (c) Statement Regarding Federally Sponsored Research and Development: See MPEP § 310.
- (d) Incorporation-By-Reference Of Material Submitted On a Compact Disc: The specification is required to include an incorporation-by-reference of electronic documents that are to become part of the permanent United States Patent and Trademark Office records in the file of a patent application. See 37 CFR 1.52(e) and MPEP § 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text were permitted as electronic documents on compact discs beginning on September 8, 2000.

Art Unit: 2134

Or alternatively, Reference to a "Microfiche Appendix": See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.

- (e) Background of the Invention: See MPEP § 608.01(c). The specification should set forth the Background of the Invention in two parts:
  - (1) Field of the Invention: A statement of the field of art to which the invention pertains. This statement may include a paraphrasing of the applicable U.S. patent classification definitions of the subject matter of the claimed invention. This item may also be titled "Technical Field."
  - (2) Description of the Related Art including information disclosed under 37 CFR 1.97 and 37 CFR 1.98: A description of the related art known to the applicant and including, if applicable, references to specific related art and problems involved in the prior art which are solved by the applicant's invention. This item may also be titled "Background Art."
- (f) Brief Summary of the Invention: See MPEP § 608.01(d). A brief summary or general statement of the invention as set forth in 37 CFR 1.73. The summary is separate and distinct from the abstract and is directed toward the invention rather than the disclosure as a whole. The summary may point out the advantages of the invention or how it solves problems previously existent in the prior art (and preferably indicated in the Background of the Invention). In chemical cases it should point out in general terms the utility of the invention. If possible, the nature and gist of the invention or the inventive concept should be set forth. Objects of the invention should be treated briefly and only to the extent that they contribute to an understanding of the invention.
- (g) Brief Description of the Several Views of the Drawing(s): See MPEP § 608.01(f). A reference to and brief description of the drawing(s) as set forth in 37 CFR 1.74.
- (h) Detailed Description of the Invention: See MPEP § 608.01(g). A description of the preferred embodiment(s) of the invention as required in 37 CFR 1.71. The description should be as short and specific as is necessary to describe the invention adequately and accurately. Where elements or groups of elements, compounds, and processes, which are conventional and generally widely known in the field of the invention described and their exact nature or type is not necessary for an understanding and use of the invention by a person skilled in the art, they should not be described in detail. However, where particularly complicated subject matter is involved or where the elements, compounds, or processes may not be commonly or widely known in the field, the specification should refer to another patent or readily available publication which adequately describes the subject matter.

- (i) Claim or Claims: See 37 CFR 1.75 and MPEP § 608.01(m). The claim or claims must commence on separate sheet or electronic page (37 CFR 1.52(b)(3)). Where a claim sets forth a plurality of elements or steps, each element or step of the claim should be separated by a line indentation. There may be plural indentations to further segregate subcombinations or related steps. See 37 CFR 1.75 and MPEP § 608.01(i)-(p).
- (j) Abstract of the Disclosure: See MPEP § 608.01(f). A brief narrative of the disclosure as a whole in a single paragraph of 150 words or less commencing on a separate sheet following the claims. In an international application which has entered the national stage (37 CFR 1.491(b)), the applicant need not submit an abstract commencing on a separate sheet if an abstract was published with the international application under PCT Article 21. The abstract that appears on the cover page of the pamphlet published by the International Bureau (IB) of the World Intellectual Property Organization (WIPO) is the abstract that will be used by the USPTO. See MPEP § 1893.03(e).
- (k) Sequence Listing. See 37 CFR 1.821-1.825 and MPEP §§ 2421-2431. The requirement for a sequence listing applies to all sequences disclosed in a given application, whether the sequences are claimed or not. See MPEP § 2421.02.

### *Claim Objections*

- 7. Claims 1-12 are object to because the claims are not presented in form consistent with current U.S. practice, where method claims should consist of a series of clear, distinguishable active method steps. Further, the claims must be in the form of a single sentence without the use of bullets; however, indentation for clarity purposes can still be used.
- 8. Claim 1 is objected to because the claim contains only a single method step (choosing, line 22).
- 9. Claim 1 is objected to because the claim contains multiple periods (.) and claims must be constructed in such a way that a single sentence is formed (lines 3 and 20).

### *Claim Rejections - 35 USC § 101*

Art Unit: 2134

10. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

11. Claims 1-12 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The invention is not tangibly embodied and produces no tangible output.

***Claim Rejections - 35 USC § 112***

12. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

13. Claims 1-12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

14. Regarding claims 1-12, it is unclear what parts of the claims are intended to be limiting to the steps of “choosing” and producing. The claims should be rewritten form such that a sequence of method steps is clearly and definitively presented.

15. Regarding claim 1, the limitations of the claim recite the nature of the output, but not how the output is achieved. For instance, the claim recites that none of equations (1) and (2) can be resolved ... which is a passive limitation describing the output, as opposed to an active method step such as (an example) reciting that equations (1) and (2) are performed and if a valid result is achieved, then the factor is disregarded.

16. Regarding claim 1, the claim recites two “comprising” limitations.

Art Unit: 2134

17. Regarding claim 1, the meaning of the term “firstly” is unclear with respect to the method step.
18. Regarding claim 3, the word “especially” renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).
19. Regarding claim 4, the phrase “several hundred” is indefinite.
20. Regarding claim 5, the phrase “close to the size” is indefinite.
21. Regarding claims 6 & 7 the phrase “(should e be zero ... combined modulus)” renders the claim indefinite because it is unclear whether this is a limitation.
22. Regarding claims 6-8, the identifier “f-e” renders the claim indefinite because it is unclear whether “f-e” refers to a single identifier or represents the result of a calculation of the difference between f and e, such as “f minus e”. Claim 8 & 9 are rejected based on their dependence upon claim 7.
23. Regarding claim 9, it is unclear if “assuming” (p. 4 of the preliminary amendment) is intended to be limiting.
24. Regarding claim 10, the excessive use of “and/or” renders the claim unclear because, it is unclear which groupings of limitations are alternatives to others. For instance, there are several variations of alternatives: (f prime factors and/or (Chinese remainders of the prime factors and/or of n) and/or the m private values  $Q_{i,j}$  and of v) or (f prime factors and/or (Chinese remainders of the prime factors and/or of (n and/or the m private values  $Q_{i,j}$ )) and of v) or (f prime factors and/or (Chinese remainders of the prime factors and/or (of n and/or the m private values ( $Q_{i,j}$  and of v)))).



*Claim Rejections - 35 USC § 102*

25. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

26. Claim 1, as best understood, is rejected under 35 U.S.C. 102(b) as being anticipated by “A “Paradoxical” Identity-Based Signature Scheme Resulting from Zero-Knowledge” by Guillou et al. (Guillou). Guillou discloses producing  $f$  prime factors ( $p$  and  $q$ ) (p. 219, §3) and choosing a security parameter/ $v$ ,  $m$  base numbers/ $J$ , the size of the modulus  $n$  (by choosing  $p$  and  $q$ ) and the size of the  $f$  prime numbers/ $p$  and  $q$  (p. 219).

27. Claim 1, as best understood, is rejected under 35 U.S.C. 102(b) as being anticipated by Applied Cryptography, Second Edition by Schneier. Schneier discloses generating (producing/choosing) all values between 0 and  $2^{2048}$  (p. 151). While Schneier is silent regarding the other limitations of the claims, it is inherent that when all values between 0 and  $2^{2048}$  are chosen, the security parameter  $k$ , the  $m$  base numbers, the size of modulus  $n$  and the size of the  $f$  prime factors meeting the requirements of the claim will have been chosen.

28. Claim 1, as best understood, is rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent 5,140,634 to Guillou et al. (Guillou). Guillou discloses producing/choosing the size of  $f$  prime factors ( $a$  and  $b$ ) (col. 2, lines 15-17) and choosing a security parameter/ $p$  (col. 12,

Art Unit: 2134

lines 3-4), m base numbers/J (col. 11, line 34), the size of the modulus n (by choosing a and b) and the size of the f prime numbers/a and b (col. 2, lines 15-17 & lines 34-37).

***Conclusion***

29. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. - 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

**Any response to this action should be mailed to:**

Commissioner of Patents and Trademarks  
Washington, DC 20231

**Or faxed to:**

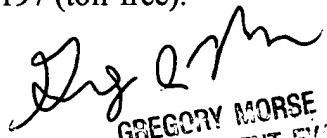
(703)746-7239 (for formal communications intended for entry)

**Or:**

(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

Application/Control Number: 09/869,966

Page 10

Art Unit: 2134

A handwritten signature in black ink, appearing to be 'MJS', written in a cursive style.

MJS

March 1, 2005